Daily brief, Monday, July 20, 2026

Jul 19, 8:00 PM to Jul 20, 8:00 PM ET

Generated Nov 3, 2026, 12:59 PM ET

0	0	0	42	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

42 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

42

9.6 **CVE-2026-15899** Google chrome

Use after free in CameraCapture in Google Chrome on Mac prior to 150.0.7871.128 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-15900** Google chrome

Use after free in GPU in Google Chrome on Android prior to 150.0.7871.128 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-15901** Google chrome

Use after free in Network in Google Chrome prior to 150.0.7871.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)

10.0 **CVE-2026-44359**

Meshtastic is an open source mesh networking solution. Prior to version 2.7.21.1370b23, the Meshtastic GitHub repository's main_matrix.yml workflow is triggered by pull_request_target and multiple jobs check out the attacker's fork code and execute it with acc

10.0 **CVE-2026-46412**

@beproduct/nestjs-auth is a NestJS authentication module for BeProduct IDS (Identity Server) with OpenID Connect support. Between 2026-05-11 20:19 UTC and 22:56 UTC, an attacker used a compromised npm publish token to publish 18 malicious versions of `@beprodu

10.0 **CVE-2026-61424**

Joomla Extension - dj-extensions.com - Unauthenticated arbitrary file upload in DJ-Classifieds < 3.11.2 - The Joomla extension DJ-Classifieds is vulnerable to an unauthenticated file upload, leading to full RCE.

10.0 **CVE-2026-61900**

Joomla Extension - dj-extensions.com - Unauthenticated arbitrary file upload in DJ-jDownloads < 4.1.6 - The Joomla extension JDownloads is vulnerable to an unauthenticated file upload, leading to full RCE.

9.9 **CVE-2026-51027**

An issue in FileThingie v.2.5.7 allows a remote attacker to obtain sensitive information via the ft2.php component.

9.9 **CVE-2026-54051**

Network-AI is a TypeScript/Node.js multi-agent orchestrator. Prior to version 5.9.1, the agent sandbox gates shell commands behind an allowlist (`SandboxPolicy.isCommandAllowed`), which THREAT_MODEL.md calls the main control against a compromised agent (Advers

9.8 **CVE-2026-16235**

Crypt::Password versions through 0.28 for Perl generate insecure random values for salts. These versions use the built-in rand function, which is predictable and unsuitable for cryptography.

9.8 **CVE-2026-64620** Freerdp freerdp

FreeRDP before 3.28.0 (affected <=3.27.1) contains a heap-based buffer overflow in crypto_rsa_common() (libfreerdp/crypto/crypto.c). The function writes the modular-exponentiation result into the caller's output buffer via BN_bn2bin() and only afterward checks

9.8 **CVE-2026-53405** Apache syncope

+2 more CVEs in the same release

Improper Isolation or Compartmentalization vulnerability in Apache Syncope. An administrator with adequate entitlements can import arbitrary BPMN process definitions via the REST API and then start the process. When a BPMN process containing a Groovy scriptTas

9.8 **CVE-2026-57308** Apache syncope

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Syncope. An administrator with adequate entitlements can achieve execution of arbitrary SQL via stacked queries, leveraging unsanitized sort parameters

9.8 **CVE-2026-62183** Apache syncope

Improper Privilege Management vulnerability in Apache Syncope. When: * the all-Java user workflow adapter is configured, or * the Flowable user workflow adapter is configured, bearing a BPMN definition not requiring admin approval for user self registration of

9.8 **CVE-2026-35048**

The Piwigo installer in versions 16.3.0 and earlier accepts POST parameters for database configuration and writes them directly into a PHP configuration file without proper sanitization. On PHP 8+, the `addslashes()` protection is bypassed because it checks fo

9.8 **CVE-2026-41252** Neutrinolabs xrdp

xrdp is an open source RDP server. Versions 0.10.6 and prior contain a missing bounds check in xrdp, which allows a heap-based buffer overflow when operating in vnc-any mode. The issue occurs during the handling of RFB protocol color map messages from a VNC se

9.8 **CVE-2026-64193**

Net::DNS versions through 1.55 for Perl allow remote execution injection via EDNS EXTENDED ERROR. Net::DNS::RR::OPT::EXTENDED_ERROR::_decompose parses the EXTRA-TEXT field of an EDNS EXTENDED-ERROR option (RFC 8914) by tokenising the raw bytes and passing the

9.8 **CVE-2026-63766**

GPT-SoVITS through 20250606v2pro contains an OS command injection vulnerability in webui.py where ASR, slice, denoise, and uvr5 functions interpolate unsanitized Gradio textbox values directly into shell commands executed with shell=True. Attackers can inject

9.8 **CVE-2026-63767**

ktransformers through 0.6.3, fixed in commit def0f93, contains an unauthenticated pickle deserialization vulnerability that allows remote attackers to execute arbitrary commands by sending crafted pickle payloads to the SchedulerServer ZMQ ROUTER socket bound

9.8 **CVE-2024-51311**

The Tenda TX9 V22.03.02.05 firmware has a stack overflow vulnerability in the sub_4418CC function of the file /goform/SetNetControlList.

20 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Suno suno.com 55,282,226 accounts

Watch Floor collects CVE records, CISA KEV, exploit indexes, official advisories, security news and chatter. CVSS is the headline score. Ransomware posts are criminal groups' claims, not confirmed by the victims. CVE IDs link to the full record on Watch Floor.